

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-100068

(43)Date of publication of application : 07.04.2000

(51)Int.Cl.

G11B 20/10

(21)Application number : 10-266715

(71)Applicant : VICTOR CO OF JAPAN LTD

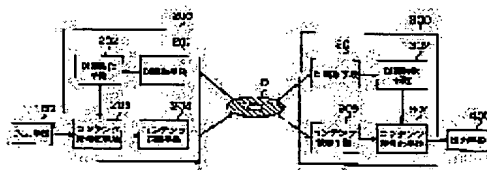
(22)Date of filing : 21.09.1998

(72)Inventor : HIRATA ATSUMI
MIYAZAKI TAKESHI
SUZUKI HIDEO**(54) INFORMATION RECORDING METHOD AND DEVICE THEREOF, INFORMATION REPRODUCING DEVICE, INFORMATION PROTECTING METHOD AND INFORMATION RECORDING MEDIUM**

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the unauthorized copy and to permit the reproduction of a properly recorded disk even by any reproducing device by keeping the intrinsic information respectively peculiar for each information recording medium to record on respective information recording media by the unchangeable method and enciphering the information while taking this intrinsic information as a key to record it on the information recording medium.

SOLUTION: When the contents CT are inputted by an input means 100, the intrinsic information DI of the disk D is read by a DI reading means 201 and made to have the functional relation by a DI functioning means 202 to define as $F(DI)$. Then, the contents CT are enciphered by the intrinsic information $F(DI)$ made to have the functional relation to define as $E(CT)$ in a contents enciphering means $F(DI)$ and recording on the disk D by a contents recording means 204. Since the peculiar intrinsic information is previously kept to record and the contents are enciphered by this intrinsic information, the intrinsic information is recorded respectively on the information recording medium, and the contents are reproducible even by the separate reproducing means.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office



6 2 0 0 0 0 2 2 0 0 0 0 1 0 0 0 6 8

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-100068

(P2000-100068A)

(43) 公開日 平成12年4月7日 (2000.4.7)

(51) Int.Cl.⁷

G 1 1 B 20/10

識別記号

F I

G 1 1 B 20/10

テーマコード* (参考)

H 5 D 0 4 4

審査請求 未請求 請求項の数 6 O L (全 11 頁)

(21) 出願番号 特願平10-266715

(22) 出願日 平成10年9月21日 (1998.9.21)

(71) 出願人 000004329

日本ビクター株式会社

神奈川県横浜市神奈川区守屋町3丁目12番地

(72) 発明者 平田 渥美

神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

(72) 発明者 宮崎 健

神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

(74) 代理人 100083806

弁理士 三好 秀和 (外9名)

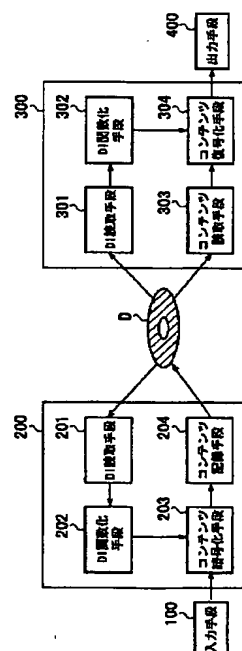
最終頁に続く

(54) 【発明の名称】 情報記録方法、その装置、情報再生装置、情報保護方法及び情報記録媒体

(57) 【要約】

【課題】 情報を放送や通信手段を介して伝達し記録型ディスクに記録する際、記録型ディスク媒体から不正にコピーされることを防止することを課題とする。

【解決手段】 ディスクDに記録された各ディスクそれぞれ特有の固有情報D Iによりコンテンツを暗号化してディスクDに記録し、再生する場合にはディスクDに記録されている固有情報D Iによって暗号化されたコンテンツを復号化することを特徴とする。



1

【特許請求の範囲】

【請求項 1】 それぞれ特有の固有情報を改変できない方法でそれぞれの情報記録媒体に記録しておき、この固有情報を鍵として情報を暗号化して前記情報記録媒体に記録することを特徴とする情報記録方法。

【請求項 2】 情報記録媒体に情報を暗号化して記録する情報記録装置であって、少なくとも前記情報記録媒体毎にそれぞれ記録された固有情報を読み取る固有情報読み取り手段と、

この固有情報読み取り手段によって読み取られた固有情報によって入力されたコンテンツを暗号化するコンテンツ暗号化手段と、

このコンテンツ暗号化手段によって暗号化されたコンテンツを前記情報記録媒体に記録するコンテンツ記録手段とから構成されることを特徴とする情報記録装置。

【請求項 3】 情報記録媒体に記録された情報を復号化して再生する情報再生装置であって、少なくとも前記情報記録媒体毎にそれぞれ記録された固有情報を読み取る固有情報読み取り手段と、

前記情報記録媒体に記録された暗号化されたコンテンツを読み取るコンテンツ読み取り手段と、

このコンテンツ読み取り手段によって読み取られた前記暗号化されたコンテンツを前記固有情報によって復号化して出力するコンテンツ復号化手段とから構成されることを特徴とする情報再生装置。

【請求項 4】 それぞれ特有の固有情報を改変できない方法でそれぞれの情報記録媒体に記録しておき、この固有情報を鍵として情報を暗号化して前記情報記録媒体に記録し、この暗号化して記録された情報を前記固有情報によって復号して再生することを特徴とする情報保護方法。

【請求項 5】 前記固有情報と認証用の情報とから認証子を生成し、前記情報記録媒体に記録されている認証子と同一であるか否かを判断することをさらに含むことを特徴とする請求項 4 に記載の情報保護方法。

【請求項 6】 各情報記録媒体毎にそれぞれ特有の固有情報が改変できない方法で、あるいは改変できないエリアに記録されていることを特徴とする情報記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、記録型ディスクに記録された情報を保護するための情報保護装置及びその方法に関し、特に個々のディスクに特有の固有情報をディスクに記録することによって、不正コピーを防止する情報を保護する方法に関する。

【0002】

【従来の技術】CD-R、PD、DVD-RAM、DVD-RWなどの記録型ディスク媒体（以下ディスクという）及び装置において、ネットワークあるいは放送を介して伝送され、正当に権利を得て 1 回記録することを許

2

された場合、映画などの動画像、静止画像、音楽などのコンテンツは簡単に記録することができなければならない。また、記録後のディスクは、正規の装置であればどの装置を利用しても再生できるようにしたいという要求がある。

【0003】一方、そのような記録型ディスク媒体及び装置において、不正にコピーされることを防止して著作権を守る必要があるが、正当な権利で容易に記録・再生できることとコピーを防止することは背反しており両立させることが困難であった。

【0004】そこで、このような矛盾を解決すべく従来の情報保護装置では、ユーザー ID を利用することによって不正なコピーを防止していた。

【0005】図 6 に示すように、従来の情報保護装置は、動画像、静止画像、音楽などのコンテンツを入力する入力手段 10 と、一般的な情報記録媒体 D にコンテンツなどの情報を暗号化して記録する情報記録手段 20 と、情報記録媒体 D に記録された情報を復号化して再生する情報再生手段 30 と、復号化されたコンテンツなどの情報を出力する出力手段 40 とを含んでいる。

【0006】ここで、情報記録手段 20 は、情報再生手段 30 からネットワーク 50 を介して送られてくるユーザー ID (UI) を読み取る UI 読み取り手段 21 と、入力手段 10 により入力されるコンテンツを暗号化するための鍵 KEY を保持する鍵保持手段 22 と、この鍵保持手段 22 に保持された鍵 KEY を UI 読み取り手段 21 によって読み取られたユーザー ID によって暗号化する鍵暗号化手段 23 と、この鍵暗号化手段 23 によって暗号化された鍵 E (KEY) をネットワーク 50 を介して情報記録媒体 D に記録する鍵記録手段 24 と、鍵保持手段 22 に保持された鍵 KEY によって入力手段 10 から入力されたコンテンツ CT を暗号化するコンテンツ暗号化手段 25 と、このコンテンツ暗号化手段 25 によって暗号化されたコンテンツ E (CT) をネットワーク 50 を介して情報記録媒体 D に記録するコンテンツ記録手段 26 とから構成されている。

【0007】また、情報再生手段 30 は、ユーザー ID (UI) を保持し、ネットワークを介して伝送する UI 保持手段 31 と、情報記録媒体 D に記録された暗号化された鍵 E (KEY) を読み取る鍵読み取り手段 32 と、この鍵読み取り手段 32 によって読み取られた暗号化された鍵 E (KEY) をユーザー ID によって復号化する鍵復号化手段 33 と、復号化された鍵を保持する鍵保持手段 34 と、情報記録媒体 D に記録された暗号化されたコンテンツ E (CT) を読み取るコンテンツ読み取り手段 35 と、このコンテンツ読み取り手段 35 によって読み取られた暗号化されたコンテンツ E (CT) を鍵保持手段 34 に保持された鍵 KEY によって復号化して出力手段 40 へ出力するコンテンツ復号化手段 36 とから構成されている。

3

【0008】次に従来の情報保護装置の動作を説明する。

【0009】コンテンツCTが入力手段10より入力されると、コンテンツ暗号化手段25において、コンテンツCTは鍵保持手段22に保持されている鍵KEYによって暗号化されてE(CT)となり、コンテンツ記録手段26によってネットワーク50を介してディスクDに記録される。

【0010】一方、ユーザーがそれぞれ固有に持つユーザーID(UI)はネットワーク50を介してUI保持手段31からUI読み取り手段21に送られ、鍵暗号化手段23において、鍵保持手段22に保持された鍵KEYを暗号化してE(KEY)とする。この暗号化された鍵E(KEY)は鍵記録手段24によってネットワーク50を介してディスクDに記録される。

【0011】そして、ユーザーは情報再生手段30において、ディスクDを再生する。まずディスクDから鍵読み取り手段32によって暗号化された鍵E(KEY)が読み取られ、次に鍵復号化手段33において暗号化された鍵E(KEY)をユーザーIDによって復号化して鍵KEYを得て鍵保持手段34に保持する。また、暗号化されたコンテンツE(CT)はコンテンツ読み取り手段35によって読み取られ、コンテンツ復号化手段36において、鍵保持手段34に保持されている鍵KEYにより復号化されてコンテンツCTとなり、出力手段40に送られ出力されることになる。

【0012】

【発明が解決しようとする課題】しかしながら、このような従来の情報保護装置では、情報再生手段30に特有のユーザーIDによって鍵KEYを暗号化してディスクDに記録していたため、ディスクDは他の情報再生手段ではユーザーIDが異なるため再生することができず、例えばユーザーが情報再生手段であるプレーヤーを買い換えた場合や増設した場合にディスクDを再生することができないという問題点があった。

【0013】そこで、他のプレーヤーでも再生できるようにユーザーIDをディスクDに記録することが考えられる。

【0014】しかしながら、ユーザーIDをディスクに記録すると、確かに図7の点線で示すようにUI保持手段31がディスクDからユーザーIDを読み取ることによって他のプレーヤでもディスクDを再生できるようにはなるものの、ディスクDを丸ごとコピーすることによって不正なコピーディスクD'が容易に作れることになり情報の保護ができなくなるという別の問題点が生じるようになっていた。

【0015】本発明は上記事情に鑑みてなされたものであり、その目的は、ネットワークあるいは放送を介して伝送されたコンテンツを正当に認められた権利によって記録したディスクから、別のディスクや記録媒体に不正

4

コピーすることを防止するとともに、正当に記録したディスクはどの再生装置でも再生することのできる情報保護装置、その方法及び情報保護するための情報記録媒体を提供することにある。

【0016】

【課題を解決するための手段】上記目的を達成するために、第1の発明である情報記録方法は、各情報記録媒体にそれぞれ特有の固有情報を改変できない方法でそれぞれの情報記録媒体に記録しておき、この固有情報を鍵として情報を暗号化して前記情報記録媒体に記録することを特徴とする。

【0017】この第1の発明によれば、不正コピーを防止できるとともに、正当に記録したディスクはどの再生装置においても再生することができる。

【0018】第2の発明である情報記録装置は、情報記録媒体に情報を暗号化して記録する情報記録装置であって、前記情報記録媒体毎にそれぞれ記録された固有情報を読み取る固有情報読み取り手段と、この固有情報読み取り手段によって読み取られた固有情報によって入力されたコンテンツを暗号化するコンテンツ暗号化手段と、このコンテンツ暗号化手段によって暗号化されたコンテンツを前記情報記録媒体に記録するコンテンツ記録手段とから構成されることを特徴とする。

【0019】この第2の発明によれば、不正コピーを防止できるとともに、正当に記録したディスクはどの再生装置においても再生することができる。

【0020】第3の発明である情報再生装置は、情報記録媒体に記録された情報を復号化して再生する情報再生装置であって、前記情報記録媒体毎にそれぞれ記録された固有情報を読み取る固有情報読み取り手段と、前記情報記録媒体に記録された暗号化されたコンテンツを読み取るコンテンツ読み取り手段と、このコンテンツ読み取り手段によって読み取られた前記暗号化されたコンテンツを前記固有情報によって復号化して出力するコンテンツ復号化手段とから構成されることを特徴とする。

【0021】この第3の発明によれば、不正コピーを防止できるとともに、正当に記録したディスクはどの再生装置においても再生することができる。

【0022】第4の発明である情報保護方法は、各情報記録媒体にそれぞれ特有の固有情報を改変できない方法でそれぞれの情報記録媒体に記録しておき、この固有情報を鍵として情報を暗号化して前記情報記録媒体に記録し、この暗号化して記録された情報を前記固有情報によって復号して再生することを特徴とする。

【0023】この第4の発明によれば、不正コピーを防止できるとともに、正当に記録したディスクはどの再生装置においても再生することができる。

【0024】第5の発明である情報保護方法は、前記固有情報と認証用の情報とから認証子を生成し、前記情報記録媒体に記録されている認証子と同一であるか否かを

5

判断することをさらに含むことを特徴とする。

【0025】この第5の発明によれば、認証子が同一であるか否かを判断することにより固有情報に変更された場合でも検出することができるので、不正なコピーをさらに防止することができる。

【0026】第6の発明である情報記録媒体は、各情報記録媒体毎にそれぞれ特有の固有情報が改変できない方法で、あるいは改変できないエリアに記録されていることを特徴とする情報記録媒体。

【0027】この第6の発明によれば、不正コピーを防止できるとともに、正当に記録したディスクはどの再生装置においても再生することができる。

【0028】

【発明の実施の形態】以下、本発明に係る情報保護装置の第1の実施形態を図面に基いて説明する。本実施形態の情報保護装置は、各情報記録媒体にそれぞれ特有の固有情報をあらかじめ記録しておき、この固有情報によってコンテンツを暗号化するものである。

【0029】図1は本実施形態の情報保護装置の構成を示すブロック図である。図1に示すように、本実施形態の情報保護装置は、動画像、静止画像、音楽などのコンテンツを入力する入力手段100と、一般的な情報記録媒体Dにコンテンツなどの情報を暗号化して記録する情報記録手段200と、情報記録媒体に記録された情報を復号化して再生する情報再生手段300と、復号化されたコンテンツなどの情報を出力する出力手段400とを含んでいる。

【0030】ここで、情報記録手段200は、情報記録媒体D毎にそれぞれ記録された固有情報DIを読み取るDI読み取り手段201と、このDI読み取り手段201によって読み取られた固有情報DIを関数化するDI関数化手段202と、このDI関数化手段202によって関数化された固有情報F(DI)によって入力手段100から入力されたコンテンツCTを暗号化するコンテンツ暗号化手段203と、このコンテンツ暗号化手段203によって暗号化されたコンテンツE(CT)を情報記録媒体Dに記録するコンテンツ記録手段204とから構成されている。

【0031】また情報再生手段300は、情報記録媒体D毎にそれぞれ記録された固有情報DIを読み取るDI読み取り手段301と、このDI読み取り手段301によって読み取られた固有情報DIを関数化するDI関数化手段302と、情報記録媒体Dに記録された暗号化されたコンテンツE(CT)を読み取るコンテンツ読み取り手段303と、このコンテンツ読み取り手段303によって読み取られた暗号化されたコンテンツE(CT)を関数化された固有情報F(DI)によって復号化して出力手段400へ出力するコンテンツ復号化手段304とから構成されている。

【0032】次に、本実施形態の情報保護装置の動作に

6

ついて説明する。

【0033】まず、コンテンツCTが入力手段100より入力されると、ディスクDの固有情報DIをDI読み取り手段201が読み取り、この固有情報DIをDI関数化手段202で関数化してF(DI)とする。そして、コンテンツ暗号化手段203において、入力されたコンテンツCTを関数化された固有情報F(DI)で暗号化してE(CT)とし、コンテンツ記録手段204によってディスクDに記録する。

【0034】そして、ユーザーは情報再生手段300においてディスクDを再生する場合には、まずディスクDからDI読み取り手段301によってディスクDの固有情報DIを読み取り、この固有情報DIをDI関数化手段302で関数化してF(DI)とする。そして、次に暗号化されたコンテンツE(CT)をコンテンツ読み取り手段303によってディスクDから読み取り、コンテンツ復号化手段304において関数化された固有情報F(DI)によって復号化してコンテンツCTとし、出力手段400に送り、出力することになる。

【0035】尚、本実施形態ではDI関数化手段202によって固有情報DIを関数化し、この関数化された固有情報F(DI)によってコンテンツCTを暗号化しているが、固有情報DIを関数化せずに直接固有情報DIによってコンテンツCTを暗号化することもできる。この場合には情報再生手段300においても固有情報DIを関数化することなく、固有情報DIによってコンテンツCTを復号化する。

【0036】このように、本実施形態の情報保護装置では、各情報記録媒体にそれぞれ特有の固有情報をあらかじめ記録しておき、この固有情報によってコンテンツを暗号化するので、ユーザーが情報再生手段を買い換えたり増設した場合でも、固有情報は情報記録媒体にそれぞれ記録されているので、別の情報再生手段でもコンテンツを再生することができる。

【0037】また、不正なコピーディスクを作成しようとして、ディスクを丸ごとコピーしたとしても、コピーされたディスクを再生しようすると、固有情報は各ディスク毎に特有のものであるから、暗号化されたときの固有情報と復号化するときの固有情報が異なってしまうためにコンテンツを復号することができない。従って、不正なコピーディスクの作成を防止することもできる。

【0038】ここで、このような本実施形態の情報保護装置の効果を発揮させるためには、情報記録媒体に記録されている固有情報DIが容易に改竄できない方法で記録されていなければならない。そこで、この固有情報DIについて説明する。

【0039】同心円状あるいはスパイラル状に情報を記録する任意の追記型あるいは書換型の一般的な情報記録媒体（以下、ディスク媒体と証する）は、図2に示すように、一般利用者は記録することができない領域、すな

7

わちBCA（バースト・カッティング・エリア）3やリードインエリア2などとユーザーが記録できる領域、データエリア1などで構成されることが多い。このようなディスク媒体において、固有情報DI（番号・記号・文字・データなど任意の形態でよい）を特定のエリアに記録するか、あるいは例えばディスク媒体生産時に記録しておく方式を用いることによって、ディスク媒体それぞれを識別することが可能となる。

【0040】ここで、固有情報DIとは、各ディスク媒体をそれぞれ識別可能な唯一、あるいは他のディスク媒体の固有情報DIとは容易に一致しない情報のことである。また、特定のエリアとは、例えば図2のBCA（バースト・カッティング・エリア）3、リードインエリア2、データエリア1などに記録することができるが、これらの場所に限らず任意の場所に記録することができるものである。

【0041】このような固有情報DIは、ユーザーが記録できない、あるいは記録されているものを改竄できない方法で記録することが必要であり、例えばディスク上に機械的な凹凸であらかじめ記録しておいたり、強いレーザー光のオンオフなどでディスクの微小領域の組成や破壊による反射率の変化で記録したり、あらかじめ機械的に記録されている信号の一部を破壊するなどの方法で記録することができる。

【0042】次に、本発明に係る情報保護装置の第2の実施形態を図面に基いて説明する。本実施形態の情報保護装置は、固有情報とは別の鍵を使ってコンテンツを暗号化するものである。

【0043】図3は本実施形態の情報保護装置の構成を示すブロック図である。図3に示すように、本実施形態の情報保護装置は、動画像、静止画像、音楽などのコンテンツを入力する入力手段100と、一般的な情報記録媒体Dにコンテンツなどの情報を暗号化して記録する情報記録手段200と、情報記録媒体に記録された情報を復号化して再生する情報再生手段300と、復号化されたコンテンツなどの情報を出力する出力手段400とを含んでいる。

【0044】ここで、情報記録手段200は、情報記録媒体D毎にそれぞれ記録された固有情報DIを読み取るDI読み取り手段201と、このDI読み取り手段201によって読み取られた固有情報DIを関数化するDI関数化手段202と、入力されるコンテンツCTを暗号化するための鍵KEYを保持する鍵保持手段205と、この鍵保持手段205により保持された鍵KEYを関数化された固有情報F(DI)によって暗号化する鍵暗号化手段206と、この鍵暗号化手段206によって暗号化された鍵E(KEY)を情報記録媒体Dに記録する鍵記録手段207と、鍵保持手段205により保持された鍵KEYによって入力手段100から入力されたコンテンツCTを暗号化するコンテンツ暗号化手段203と、この

8

コンテンツ暗号化手段203によって暗号化されたコンテンツE(CT)を情報記録媒体Dに記録するコンテンツ記録手段204とから構成されている。

【0045】また情報再生手段300は、情報記録媒体D毎にそれぞれ記録された固有情報DIを読み取るDI読み取り手段301と、このDI読み取り手段301によって読み取られた固有情報DIを関数化するDI関数化手段302と、情報記録媒体Dに記録された暗号化された鍵E(KEY)を読み取る鍵読み取り手段305と、暗号化された鍵E(KEY)を関数化された固有情報F(DI)によって復号化する鍵復号化手段306と、この鍵復号化手段306によって復号化された鍵KEYを保持する鍵保持手段307と、コンテンツ記録手段204によって情報記録媒体Dに記録された暗号化されたコンテンツE(CT)を読み取るコンテンツ読み取り手段303と、暗号化されたコンテンツE(CT)を鍵保持手段307に保持された鍵KEYによって復号化して出力手段400へ出力するコンテンツ復号化手段304とから構成されている。

【0046】次に、本実施形態の情報保護装置の動作について説明する。

【0047】まず、コンテンツCTが入力手段100より入力されると、コンテンツ暗号化手段203において、入力されたコンテンツCTを鍵保持手段205に保持された鍵KEYによって暗号化してE(CT)とし、コンテンツ記録手段204によってディスクDに記録する。一方、DI読み取り手段201ではディスクDの固有情報DIを読み取り、この固有情報DIをDI関数化手段202で関数化してF(DI)とする。そして、鍵暗号化手段206において、鍵保持手段205で保持された鍵KEYを暗号化してE(KEY)とし、鍵記録手段207によってディスクDに記録する。

【0048】そして、ユーザーは情報再生手段300においてディスクDを再生する場合には、まずディスクDからDI読み取り手段301によってディスクDの固有情報DIを読み取り、この固有情報DIをDI関数化手段302で関数化してF(DI)とする。そして、鍵読み取り手段305によって読み取られた暗号化された鍵E(KEY)を、鍵復号化手段306において関数化された固有情報F(DI)で復号化して鍵KEYとし、鍵保持手段307に保持する。

【0049】一方、暗号化されたコンテンツE(CT)はコンテンツ読み取り手段303によってディスクDから読み取られ、コンテンツ復号化手段304において鍵保持手段307に保持された鍵KEYによって復号化してコンテンツCTとし、出力手段400に送られ出力されることになる。

【0050】尚、本実施形態ではDI関数化手段202によって固有情報DIを関数化し、この関数化された固有情報F(DI)によってコンテンツCTを暗号化してい

るが、固有情報DIを関数化せずに直接固有情報DIによってコンテンツCTを暗号化することもできる。この場合には情報再生手段300においても固有情報DIを関数化することなく、固有情報DIによってコンテンツCTを復号化する。

【0051】このように、第2の実施形態の情報保護装置では、固有情報によってコンテンツを暗号化するのではなく、別に保持されている鍵でコンテンツを暗号化し、この鍵を固有情報で暗号化するので、第1の実施形態の情報保護装置と同様にユーザーが情報再生手段を買

い換えたり増設した場合でもコンテンツを再生することができ、不正なコピーディスクの作成も防止できるとともに、さらに情報の保護が確実となる。

【0052】また、図1と図3に示す第1及び第2の実施形態の情報保護装置において、ネットワーク（放送型、ポイント・ツー・ポイント型、バスラインなど任意の形態を含む）を介してコンテンツを伝送する場合について、図4、図5にそれぞれ示す。基本的な構成は図1、図3と同じでディスクDに記録する際にネットワーク500が介在する。

【0053】次に、情報記録媒体に固有情報DIだけでなく認証子を記録する場合について説明する。

【0054】追記型ディスク媒体では、ある物理アドレスに一度記録したデータは破壊することはできても、その同じ物理アドレスに異なるデータを記録することはできないので改竄される心配はないが、書き換え可能のディスクの場合にはある物理アドレスに記録した固有情報を故意あるいは不意に変更されてしまうことがあるので固有情報の改竄が問題となる。

```

"12345678 9abcdef0 12345678 9abcdef0 12345678 9abcdef0
12345678 9abcdef0 12345678 9abcdef0 12345678 9abcdef0
12345678 9abcdef0 12345678 9abcdef0"

```

がリードインエリアの一部または全部であるとして、こ

```

"12345678 9abcdef0 12345678 9abcdef0 12345678 9abcdef0
12345678 9abcdef0 12345678 9abcdef0 12345678 9abcdef0
12345678 9abcdef0 12345678 9abcdef0
fedcba98 76543210"

```

これを関数の入力とする。

【0058】ここで、入力する関数がハッシュ関数 S

```

"f18ea0b5 a80901bf d348fa03 4c173b88 eb4e2191"

```

となる。この認証子をデータエリア内に記録する。例えば、当該固有情報がデータエリア最終セクタ先頭に記録されていると仮定し、それに続いて同じセクタ内に、この認証子を記録しておくこともできる。

【0059】次に、このように記録された認証子を利用して、固有情報が変更されていないか検査する。まず、ある特定エリアにある当該固有情報と、ある特定エリアにある認証用の別の情報とをある関数に入力する。そして、その関数の出力値がある特定エリアにある認証子と等しくなれば、記録されている固有情報は正しいと認証

【0055】この問題点を解決するために、固有情報と認証用の別の情報とに適当な関数を作動させて、その関数値、すなわちその関数の出力値を認証子として特定のエリアに記録する。固有情報が変更されている場合には認証子が異なってしまうため、固有情報が変更されたことを検出することができる。

【0056】この方法に用いることができる関数は、固有情報が増加すると出力値が変化し、さらに別の認証用の情報が変化しても出力値が変化するような関数であれば任意の関数を用いることができる。このような機能を持つ関数としては、SHA、MD5などの任意のハッシュ関数や、ブロック暗号DES、公開鍵暗号RSAなどの任意の暗号関数をCBC（サイファブロックチェーン）モード、OFB（アウトプットフィードバック）モード、CFB（サイファフィードバック）モードなどがある。また、ここで用いる関数は任意の長さの入力を扱うことができる関数を用いることもできるので、認証用の別の情報にはディスク内の任意のエリアで任意の長さの情報を使うことができる。また、この関数の出力（関数値）である認証子は、図2のBCA3（パースト・カッティング・エリア）、リードインエリア2、データエリア1などに記録することができるが、これらの場所に限らず任意の場所に記録してもよい。

【0057】ここで、認証子の具体例を説明すると、例えば当該固有の情報

```

"fedcba98 76543210"

```

が、データエリア最終セクタ先頭に記録されていて、別の認証用の情報

HA-1 [1] であると仮定すると、その出力値（認証子）は、

し、等しくなければ記録されている固有情報は誤っていると認証することができる。

【0060】また、固有情報の記録されたディスク媒体では、従来のディスク記録・再生装置においても、データエリアにあるデータを読みとるためには、ソフトウェアやファームウェアの変更のみで、ハードウェアの変更無しに読みとることができる。具体的には、例えばデータエリアの最終セクタ、あるいはこれ以上記録しないであろうという適当なセクタに固有情報を記録し、リードアウトフラグをそのセクタの前あるいはそのセクタ内の

11

先頭に記録することで実現することができる。このように、データエリアの最終セクタに固有情報を記録しておけば、再生すべきデータの後に記録することになるので、このようなディスク媒体を従来のディスク記録・再生装置で再生する場合には、何ら通常のディスクと変わらずに再生することができる。これ以上記録しないであろうという適当なセクタに固有情報を記録した場合も同様である。ただ、固有情報を最終セクタに記録した場合が最も効率が良くなり、セクタのサイズが例えば 2 K バイトの時は、データエリアが 2 K バイト小さくなるだけである。

【0061】別の方法としては、リードインエリア内にリードイン情報とは別に固有情報を記録しておくこともでき、パーストカッティングエリアに記録することもできる。ここで、パーストカッティングエリアとは、ディスク最内周に位置し、非同期で読み取ることを仮定しているエリアのことで、機能が等しければパーストカッティングエリアという名称には捕らわれないものである。

【0062】また、パーストカッティングエリアを読みとる仕様になっていない従来のディスク記録・再生装置においては、もともとパーストカッティングエリアを無視して再生するので、従来のディスク記録・再生装置で再生する場合には何ら通常のディスクと変わらずに再生することができる。

【0063】

【発明の効果】以上説明したように、本発明の情報保護装置、その方法及び情報保護するための情報記録媒体によれば、各情報記録媒体にそれぞれ特有の固有情報をあらかじめ記録しておき、この固有情報によってコンテンツを暗号化するので、ユーザーが情報再生手段を買い換えたり増設した場合でも、固有情報は情報記録媒体に記録されているので、別の情報再生手段でもコンテンツを再生することができる。

【0064】また、不正なコピーディスクを作成しようとして、ディスクを丸ごとコピーしたとしても、コピーされたディスクを再生しようとする、固有情報は各ディスク毎に特有のものであるから、暗号化されたときの固有情報と復号化するときの固有情報が異なってしまうためにコンテンツを復号することができない。従って、不正なコピーディスクの作成を防止することもできる。

【0065】さらに、固有情報だけでなく別の鍵をも利用してコンテンツを暗号化することにより、不正コピーを防止でき、正当に記録したディスクはどの再生装置においても再生できるとともに、さらに情報の保護が確実となる。

12

【0066】また、認証子が同一であるか否かを判断することにより固有情報が変更された場合でも検出することができるので、不正なコピーをさらに防止することもできる。

【図面の簡単な説明】

【図1】本発明による情報保護装置の第1の実施形態の構成を示すブロック図である。

【図2】情報記録媒体であるディスクの構成を示す図である。

【図3】本発明による情報保護装置の第2の実施形態の構成を示すブロック図である。

【図4】図1に示す情報保護装置の第1の実施形態において、ネットワークを介する場合における構成を示すブロック図である。

【図5】図3に示す情報保護装置の第2の実施形態において、ネットワークを介する場合における構成を示すブロック図である。

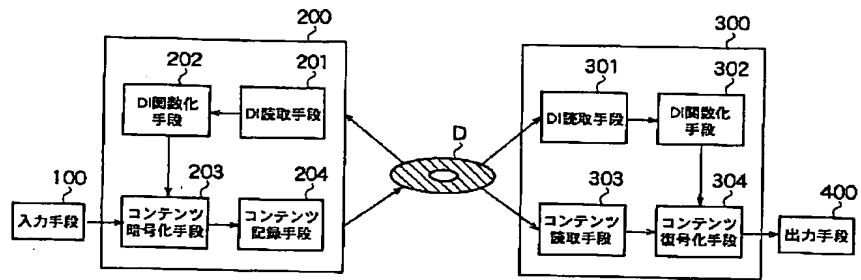
【図6】従来の情報保護装置の構成を示すブロック図である。

【図7】図6に示す従来の情報保護装置において、ユーザーIDをディスクに記録した場合を説明するためのブロック図である。

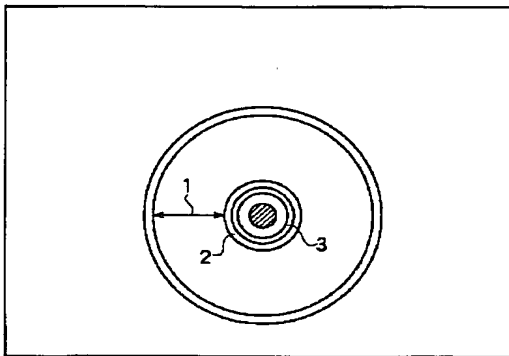
【符号の説明】

- 1 データエリア
- 2 リードインエリア
- 3 パースト・カッティング・エリア
- 10、100 入力手段
- 20、200 情報記録手段
- 21 UI読み取り手段
- 22、205 鍵保持手段
- 23、206 鍵暗号化手段
- 24、207 鍵記録手段
- 25、203 コンテンツ暗号化手段
- 26、204 コンテンツ記録手段
- 31 UI保持手段
- 32、305 鍵読み取り手段
- 33、306 鍵復号化手段
- 34、307 鍵保持手段
- 35、303 コンテンツ読み取り手段
- 36、304 コンテンツ復号化手段
- 30、300 情報再生手段
- 40、400 出力手段
- 50、500 ネットワーク
- 201、301 DI読み取り手段
- 202、302 DI関数化手段
- D 情報記録媒体

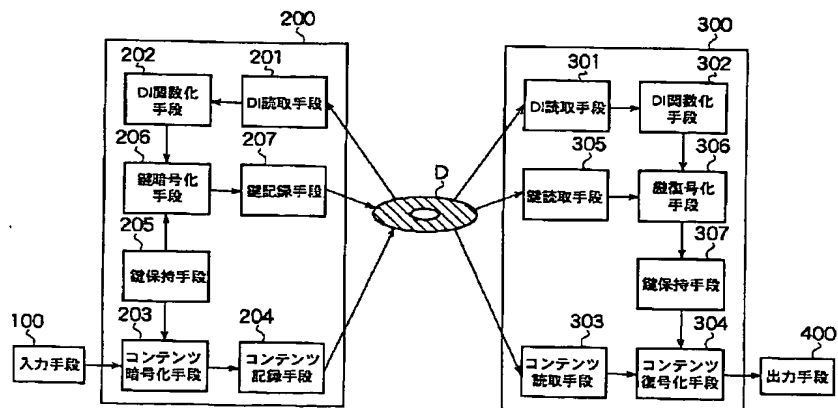
【図 1】



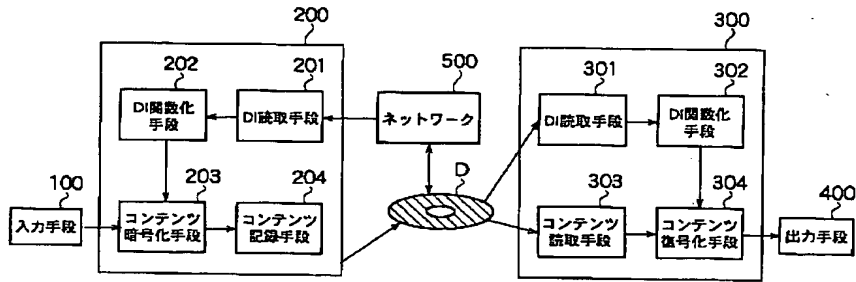
【図 2】



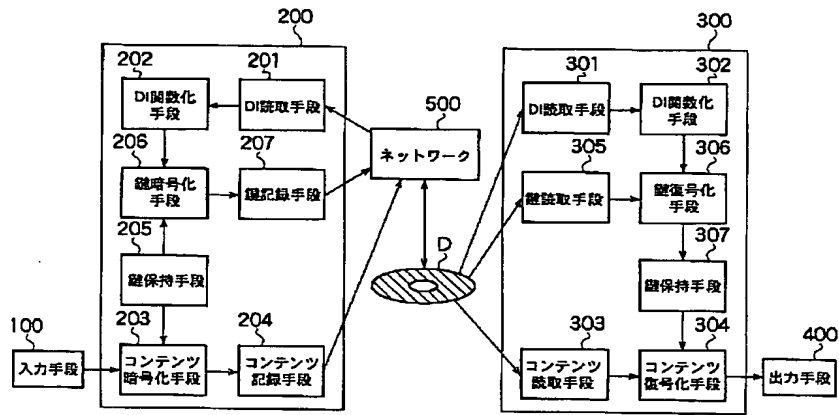
【図 3】



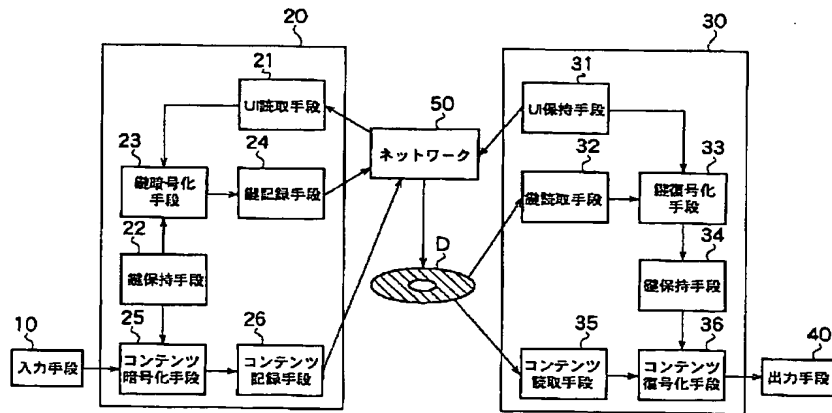
【図 4】



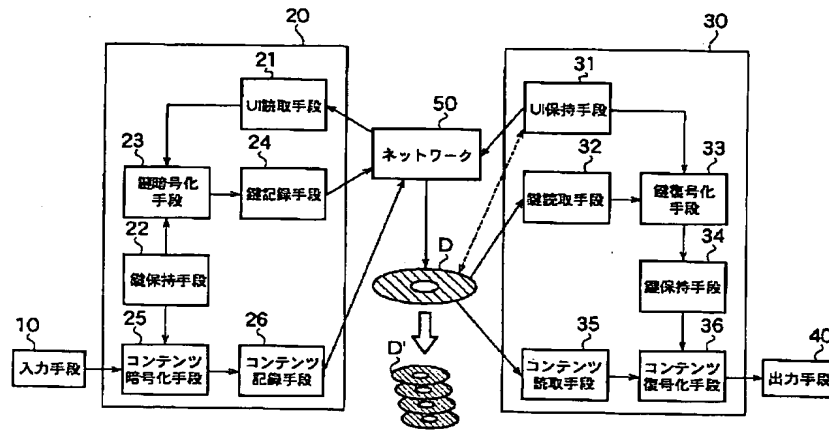
【図 5】



【図 6】



【図7】



【手続補正書】

【提出日】平成11年7月27日（1999. 7. 27）

【補正対象項目名】図1

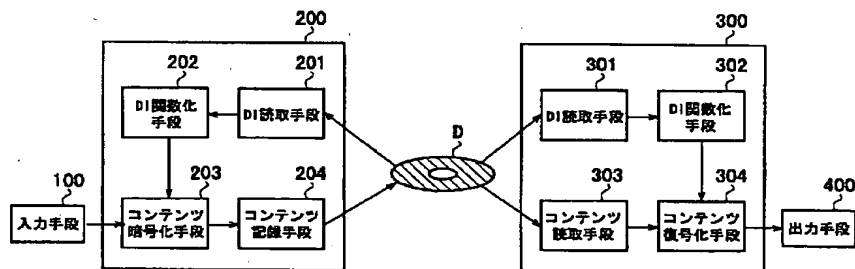
【補正方法】変更

【手続補正1】

【補正内容】

【補正対象書類名】図面

【図1】



【手続補正2】

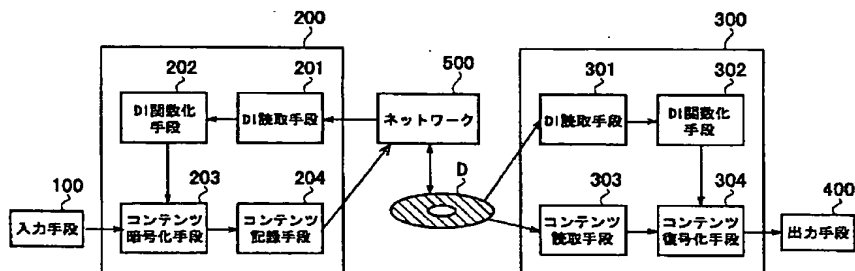
【補正方法】変更

【補正対象書類名】図面

【補正内容】

【補正対象項目名】図4

【図4】



フロントページの続き

(72)発明者 鈴木 英男

神奈川県横浜市神奈川区守屋町 3 丁目12番

地 日本ビクター株式会社内

F ターム(参考) 5D044 BC06 CC04 DE49 DE50 EF05

FG18 GK11 GK17 HL08